

Exhibit 2

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

JANE DOE 1, on behalf of herself and all
others similarly situated,

Plaintiff,

-against-

MATTHEW WEISS, LOYOLA UNIVERSITY
CHICAGO, AND KEFFER DEVELOPMENT
SERVICES, LLC,

Defendants.

Case No. 1:25-cv-04233

JURY TRIAL DEMANDED

PLAINTIFF'S CLASS ACTION COMPLAINT

Plaintiff JANE DOE 1, through her attorneys, Sommers Schwartz, P.C., Pitt McGehee Palmer Bonanni & Rivers, P.C., and Wallace Miller, for their Complaint against MATTHEW WEISS, LOYOLA UNIVERSITY CHICAGO, and KEFFER DEVELOPMENT SERVICES, LLC, states as follows:

I. INTRODUCTION

Students and alumni connected to Loyola University Chicago from 2015 to 2023—many of them student-athletes—have been subjected to a deeply troubling and unlawful breach of privacy, stemming from the actions of former University of Michigan and Baltimore Ravens football coach Matthew Weiss, whose gross and despicable violations of their privacy were facilitated by institutional negligence. This class action lawsuit, filed against Matthew Weiss, Loyola University Chicago, and Keffer Development Services, LLC, seeks justice for the unauthorized access and misuse of personal information—an abuse so severe that Loyola

University Chicago students and student-athletes are now receiving formal notification from the U.S. Department of Justice that their private information, including intimate photos and videos, have been exposed, including Plaintiff Jane Doe 1. This action is brought to hold the Defendants accountable for failing to protect their students from foreseeable harm.

II. PARTIES

1. Plaintiff Jane Doe 1 was a student athlete at Loyola University Chicago between 2014-2019 and was a member of the Volleyball Team.

2. Plaintiff Jane Doe 1 is domiciled in Florida, in the City of Jupiter.

3. On or about March 25, 2025, Plaintiff Jane Doe 1 received notice from the United States Department of Justice Victim Notification System that she was identified as a victim in the criminal case against University of Michigan's Coach Weiss: *United States v. Defendant(s) Matthew Weiss.*¹

4. Defendant Loyola University Chicago ("University") is a private university with its headquarters, domicile, and principal place of business in Chicago, Illinois.

5. Loyola University Chicago enrolls approximately 16,000 undergraduate and graduate students.

6. Loyola University Chicago is a member of the National Collegiate Athletic Association (NCAA), with over 300 student athletes competing in 16 intercollegiate sports at the Division 1 level.

7. Defendant Keffer Development Services, LLC ("Keffer") is a Pennsylvania limited liability company in Grove City, PA, that has continuously and systematically conducted business

¹ Jane Doe 1's DOJ Data Breach Notice is attached hereto as **Exhibit A.**

in Illinois by directly providing services to residents and entities within the State of Illinois, including its business contacts with Loyola University Chicago in Illinois, thereby availing itself of protections of the law of the State of Illinois.

8. Defendant Keffer is a technology and data vendor operating an electronic medical record and student athlete training system, which stored the personal identifying information (“PII”) and personal health information (“PHI”) of Plaintiff and Class Members across the country.

9. The wrongful conduct and legal violations committed by Defendant Keffer that are subsequently outlined in this Complaint occurred specifically with respect to the Plaintiff during the time of the incident alleged in this Complaint.

10. Matthew Weiss (“Weiss”) is an individual residing in the State of Michigan, who had contacts with the State of Illinois in that he conducted illegal activity in the State of Illinois, by hacking into the personal property of Plaintiff and putative Class Members of the State of Illinois during the applicable time period at issue in this Complaint and said activities from which this Complaint arises.

11. On March 20, 2025, Defendant Weiss was indicted on 24 counts of unauthorized access to computers and aggravated identity theft by the U.S. Attorney for the Eastern District of Michigan.

III. JURISDICTION AND VENUE

12. Jurisdiction is proper in this Court under 28 U.S.C. §§ 1331 and 1337 as this matter involves a claim under the Stored Communications Act, 18 U.S.C. § 2701(a) *et seq.*; the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Title IX, 20 U.S.C. § 1681(A) *et seq.*; 42 U.S.C. § 1983; the Fourth Amendment of the U.S. Constitution; and the Fourteenth Amendment of the U.S.

Constitution, and this Court has supplemental jurisdiction of all additional causes of action alleged in this Complaint pursuant to 28 U.S.C. §1367(a).

13. This Court also has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d) under the Class Action Fairness Act (“CAFA”) as a class action lawsuit in which the amount in controversy exceeds \$5,000,000.00, there are more than one-hundred putative Class Members, and the majority of the putative Class Members are citizens of a state different than the state of which Defendants are citizens.

14. The Court has personal jurisdiction over Defendants named in this action because Defendant University is located and created under the laws of the State of Illinois, and Defendant Weiss had minimum contacts with the State of Illinois as set forth above, thus purposefully availing himself of the privilege of conducting activities in the State of Illinois. Defendant Keffer conducts business at the State of Illinois and has availed itself of the protections of Illinois state law. The claims at issue in this case arise out of Defendants’ purposeful contacts with and business activities in the State of Illinois.

15. Venue is appropriate in this District Court under 28 U.S.C. §1391(b) since a substantial part of the events or omissions giving rise to these claims occurred within this District.

16. Plaintiff’s injuries are redressable by monetary compensation, and all alleged injuries of Plaintiff and Class Members can be traced to Defendants’ conduct.

IV. COMMON ALLEGATIONS

A. WEISS’S DATA BREACH AND CYBER SEXUAL ASSAULT OF THOUSANDS OF STUDENTS FOR NEARLY A DECADE AND THE ROLE DEFENDANT KEFFER AND UNIVERSITY PLAYED IN HIS SCHEME

17. Plaintiff brings this class action against Defendants University and Keffer for their failure to properly secure the highly sensitive personally identifiable information (“PII”) and

protected health information (“PHI”) of more than 150,000 students, including herself, which was targeted, accessed, and exfiltrated by former University of Michigan and Baltimore Ravens coach and sexual predator Matthew Weiss, over the course of nearly a decade.

18. Between 2015 and January 2023, Defendant Weiss gained unauthorized access to both student databases and student-athlete databases of more than 100 colleges and universities, some of which were maintained by Defendant Keffer, a third-party vendor contracted by these colleges and universities.

19. Upon information and belief, Defendant Loyola University Chicago contracted with Defendant Keffer.

20. After gaining access to these databases, Weiss downloaded the PII and PHI of more than 150,000 athletes.

21. Using the information that Weiss obtained from the student and student-athlete databases and his own research, Weiss was able to obtain access to the social media, email, and/or cloud storage accounts of more than 2,000 students. Defendant Weiss also illegally obtained access to the social media, email, and/or cloud storage accounts of more than 1,300 additional students and/or alumni from universities and colleges across the country. Once Weiss obtained access to these accounts, he downloaded personal, intimate digital photographs and videos that were never intended to be shared beyond intimate partners.

22. Defendant Weiss primarily targeted female college athletes. He researched and targeted these women based on their school affiliation, athletic history, and physical characteristics.

23. Through this scheme, unknown to students and student athletes, Defendant Weiss downloaded intimate digital photographs and videos.

24. This scheme appears to be the largest cyber sexual assault of student athletes in U.S. history.

25. The data breach and cyber sexual assault of over 150,000 students from university and college databases, including athletic databases maintained by Keffer, and the targeted exfiltration of intimate, personal, digital photographs and videos of 3,300 students and athletes, continued for nearly a decade because Defendant Loyola University Chicago and Defendant Keffer failed to prevent, detect, or stop Weiss from accessing those databases without and in excess of any authorization.

26. In at least several instances, Defendant Weiss exploited vulnerabilities in universities' account authorization processes to gain access to the accounts of students or alumni. Weiss then leveraged his access to these accounts to gain access to other social media, email, and/or cloud storage accounts.

27. That level of access through that number of accounts is an egregious and grossly negligent failure of data security on its face, as no institution with reasonable data security would allow such a breach over an eight-year period.

28. In March 2025, Matthew Weiss was charged in a 24-count indictment alleging 14 counts of unauthorized access to computers and 10 counts of aggravated identity theft, by the U.S. Attorney for the Eastern District of Michigan, for Weiss's perpetration of the cyber sexual assaults and data breach.

B. DEFENDANT KEFFER AND ITS “ATHLETIC TRAINER SYSTEM”

29. Defendant Keffer is a software development vendor that developed an electronic medical record system known as “The Athletic Trainer System,” which is used by many schools, colleges and universities across the United States.²

30. Defendant Keffer was founded in 1994 and currently collaborates with over 600 clients across 48 states and internationally.³ Defendant Keffer advertises that it currently serves over 6,500 schools, clinics, and other organizations with over 27,000 users and 2 million athletes.⁴

31. Upon information and belief, among the universities served by Keffer is Defendant University, Jane Doe 1’s alma mater.

32. Keffer represents that its Athletic Trainer System tool was “designed with athletic trainers for athletic trainers,” and is designed to store personal identifying information and personal health information belonging to students including their treatment histories, diagnoses, injuries, photos, and personal details, like height and weight, mental health information, and demographic information.⁵

33. In Keffer’s FAQ, it boasts that: “Keffer Development hosts all databases in our SSAE-16, SOC II and FedRamp certified data center” and that “Information security is a high priority in our company.”⁶ Keffer further claims that “On top of our Data Center being FedRamp Certified, ATS is also HIPAA and FERPA compliant. We utilize a company called Compliance Helper to ensure we maintain HIPAA and FERPA compliance.”⁷

² https://www.athletictrainersystem.com/pdf_files/Athlete_Info.pdf.

³ <https://www.athletictrainersystem.com/CompanyHistory.aspx>

⁴ <https://www.athletictrainersystem.com/Default.aspx>

⁵ See <https://www.athletictrainersystem.com/DemoRequest.aspx>

⁶ https://www.athletictrainersystem.com/pdf_Files/ATS_FAQ.pdf

⁷ *Id.*

34. In Keffer's Privacy Policy, it acknowledges that it has obligations as a "business associate" under HIPAA: "To the extent that KDS [Keffer] receives or maintains patient medical information in the course of providing the Clinical EMR, that information is secured, used and disclosed only in accordance with KDS' legal obligations as a "business associate" under HIPAA."⁸

35. Keffer's Privacy Policy further states: "KDS understands that storing our data in a secure manner is essential. KDS stores PII, PHI and other data using industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as unauthorized use, access, disclosure, destruction or modification. Please note, however, that while KDS has endeavored to create a secure and reliable website for users, the confidentiality of any communication or material transmitted to/from the Website or via e-mail cannot be guaranteed."⁹

36. Despite recognizing these obligations, Keffer failed to implement basic, industry standard systems to protect students' – including Jane Doe 1's personal identifying information and protected health information.

37. As an example, while Keffer maintained the option to incorporate two-factor authentication to access its Athletic Trainer System applications, it did not require that institutions and users do so.¹⁰ A two-factor basic security measure that requires an additional layer of authentication on top of a login credential, such as a code sent via text message or email – and critically, would have prevented Defendant Weiss from gaining access to student protected health information with only the access credentials belonging to other administrators and users.

⁸ https://www.athletictrainersystem.com/pdf_Files/ATS_Privacy_Policy.pdf

⁹ *Id.*

¹⁰ https://www.athletictrainersystem.com/pdf_Files/ATS_FAQ.pdf

38. Defendants knew that Keffer did not require institutions and users to use two-factor authorization to access the private information and communications accessible through its system, including information maintained in the Defendant Loyola University Chicago's facilities, and thus knowingly and deliberately permitted Plaintiff's confidential information and communications to be accessed, shared, and divulged without authorization from Plaintiffs.

39. Recent actions by the FTC underscore the gross negligence and failings of Keffer and Defendant Loyola University Chicago in failing to ensure that the Athletic Trainer System was configured to default to two-factor or multi-factor authentication for access to its systems containing personal identifying information and protected health information. In February 2023, the FTC published an article titled, *Security Principles: Addressing Underlying Causes of Risk in Complex Systems*. The article highlighted the importance of multi-factor authentication (MFA), stating: "Multi-factor authentication is widely regarded as a critical security practice because it means a compromised password alone is not enough to take over someone's account."¹¹

40. Additionally, the FTC's enforcement actions over the past five years further emphasize the critical and fundamental role MFA plays in an effective data security system, where the FTC has repeatedly obtained MFA as a form of injunctive relief in data security enforcement actions.¹²

41. Keffer also lacked any effective data auditing program to measure the download activity from its system, which would have allowed it to detect the massive, years-long data breach

¹¹<https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems>

¹² E.g., *In re: Equifax* (July 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach>; *In re Drizly* (Oct. 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million>.

on its systems by Defendant Weiss and the resulting cyber sexual assault on Plaintiff Jane Doe 1 and those Class Members similarly situated.

42. Both Keffer and Defendant Loyola University Chicago had a responsibility and duty to protect the private data of student athletes stored within their database and to have mechanisms in place to prevent such a gross invasion of privacy as what occurred in this case.

43. The risk of identity theft and breaches of security to access users' private, personal, and confidential information is foreseeable within the University and Keffer's information technology systems, and the University and Keffer are well aware of the foreseeable risks of breaches, such as those alleged in this case, that are likely to occur if their practices in detecting, preventing, and mitigating such breaches are substandard.

C. DEFENDANT UNIVERSITY'S FAILURE TO SAFEGUARD ITS STUDENTS' PRIVATE INFORMATION FOR NEARLY A DECADE

44. Defendant Loyola University Chicago is an established high-level educational institution, with a diverse athletic program, enrolling approximately 300 student athletes at any one time in 16 different sports at the NCAA Division 1 level.

45. In maintaining its athletics department and programs, Loyola University Chicago provides its student athletes with athletic trainers.

46. The University had a responsibility and duty to oversee the University's operations, policies and procedures, and to care for and protect the University's students.

47. The University was required to ensure that students, such as Jane Doe 1, were not exposed to sexual predators who would invade their privacy.

48. The University failed in this duty by failing to take any reasonable action to prevent the harm caused to Jane Doe 1 and other Class Members as alleged in this Complaint.

49. This prolific and egregious breach and violation was entirely preventable by the University and Keffer. As noted in a criminal complaint filed by the U.S. Attorney for the Eastern District of Michigan, Defendant Weiss breached Keffer's systems and the systems of colleges and universities across this nation by exploiting passwords and other vulnerabilities in the systems and authentication processes of Keffer and these universities. On information and belief, neither the University nor Keffer required that its employees or students implement safeguards like multi-factor authentication to access accounts, a standard practice for all entities collecting personal identifying information, especially medical data and PHI (protected health information).

50. The breach and cyber assaults were a direct result of Defendant Loyola University Chicago's and Keffer's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Jane Doe 1 and Class Members PII and PHI, leaving the most sensitive and personal information of students, like Jane Doe 1, vulnerable to exploitation by malicious predators like Defendant Weiss.

51. Defendant Loyola University Chicago was grossly negligent on two fronts: (1) in its hiring and oversight of Defendant Keffer and its entrusting of students' PII and PHI in the care of Defendant Keffer, and (2) in its maintenance, oversight and security of its own internal databases of those internal systems to protect student PII and PHI.

52. The University took no reasonable actions to prevent this access despite its duties to students and has taken no reasonable actions to notify or rectify harm to the victims of Matthew Weiss's misconduct and predation.

53. Thousands of students still remain at risk because the University and Keffer have failed to undertake any reasonable review of how Jane Doe 1's private and personal information is stored, maintained, and who can access such information, and from where.

54. To this day, the University has not formally informed Class Members impacted by Weiss's cyber sexual assault and misconduct.

D. LOYOLA UNIVERSITY CHICAGO WAS NEGLIGENT IN HIRING/CONTRACTING WITH DEFENDANT KEFFER AND IN ENTRUSTING STUDENTS PII AND PHI TO KEFFER

55. Defendant Loyola University Chicago provided its student athletes medical treatment, including from athletic trainer employees of the University.

56. To facilitate that treatment, the University contracted with Keffer to use its Athletic Training System application, which required that student athletes provide the University and Keffer with sensitive PII and PHI.

57. When collecting that information, the University, like Keffer, accepted an obligation to protect that information under contract and statutory principles, including as a "business associate" under HIPAA.

58. Jane Doe 1 and others similar to her entrusted that the University and Keffer would safeguard her private information and ensure the security and confidentiality of her data.

59. The University and Keffer had, and continue to have, a duty to protect Jane Doe 1 and to take appropriate security measures to protect private, personal, medical and intimate information, communications, and images.

60. The University knowingly and deliberately permitted access to and divulging of Plaintiffs' stored communications through Keffer and failed to take reasonable action to ensure that Keffer protected the privacy of the sensitive information of Jane Doe 1 and others like her.

61. Upon information and belief, the University failed to properly investigate Keffer and Keffer's protocols, and failed to adequately monitor or establish safeguards for Keffer's work

with the students and their private information to ensure they carried out their duties to safeguard and protect the private information of their students entrusted to them.

62. The University was negligent and/or reckless in failing to ensure that media and other private, personal and sensitive information, including but not limited to those of Jane Doe 1, was securely protected, as the University was entrusted to do.

63. The University failed to implement the security measures necessary to protect their students PII and PHI, including failing to train staff and employees on securing credentials, requiring multi-or-two-factor authentication to use Keffer's Athletic Trainer System, overseeing third-party vendors like Keffer, in which the University entrusted students sensitive PII and PHI and monitoring and auditing access to student files and private information.

64. In other words, the University not only failed to ensure it had implemented sufficient security protocols and procedures across its own systems and staff, but also the University failed to ensure Keffer had adequate security measures in place to protect its students' PII and PHI from theft and misuse.

65. The University lacked adequate training programs to detect and stop breaches like those caused by Defendant Weiss.

66. The University and Keffer failed to implement reasonable protective measures to detect Weiss' irregular activity and trespassing, including but not limited to, appropriate authentication tools, behavioral analytics, anomaly detection, machine learning, and real-time monitoring of user activity, looking for deviations from established patterns and suspicious actions like unusual login attempts or access to sensitive data, any of which would have prevented Weiss' improper access to private student information.

67. Because Keffer and the University failed to implement basic, industry standard security measures, together these Defendants allowed an alleged sexual predator, ex-football coach Matthew Weiss, to access students', and in particular female student athletes', most sensitive information for nearly a decade.

68. All Defendants disregarded the rights of Jane Doe 1 and Class Members. The University and Keffer knowingly, intentionally, willfully, recklessly and/or negligently provided access to and/or divulged Plaintiffs' private communications stored in their facilities; failed to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failed to disclose that they did not have adequately robust computer systems and security practices to safeguard private information; failed to take standard and reasonably available steps to prevent the data breach and cyber assault; failed to properly train their staff and employees on proper security measures; failed to provide Jane Doe 1 and the Class Members prompt notice of the data breach and cyber assault.

69. Defendants Loyola University Chicago's and Keffer's conduct amounts to a violation of the duties they owed to Jane Doe 1 under common law and state and federal statutory law, rendering them liable to Jane Doe 1 and the Class Members for the harms caused by this egregious and preventable cyber sexual assault and invasion of privacy. Defendant Weiss is equally liable for the harms inflicted on Jane Doe 1 and the Class Members by his intentional hacking and exfiltration of their private information under tort and statutory law.

70. Jane Doe 1 and the putative Class Members are current and former students at Loyola University Chicago and other affected institutions in the United States that were specifically targeted by Weiss and harmed by the violation of their privacy.

71. Jane Doe 1 and the putative Class Members suffered injury because of Defendants' conduct. These injuries included: invasion and loss of privacy, loss of dignity, humiliation, embarrassment, and severe emotional distress.

72. Jane Doe 1 seeks to remedy these harms on behalf of herself and all similarly situated individuals whose private information was accessed by Weiss.

73. Jane Doe 1 seeks remedies including, but not limited to, compensatory damages, nominal damages, punitive damages, and reimbursement of out-of-pocket costs. Jane Doe 1 also seeks injunctive and equitable relief to prevent future injury on behalf of herself and the putative Class Members.

E. JANE DOE 1'S ALLEGATIONS

74. Plaintiff Jane Doe 1 is a former student athlete at Loyola University Chicago.

75. While in school at Loyola University Chicago, Jane Doe 1 participated in the Volleyball program while Defendant Weiss's data breach and cyber sexual assault was ongoing.

76. As a student athlete, Jane Doe 1 received treatment from the University's athletic trainer staff, requiring her to disclose information about her treatment, including height, weight, injuries, medications, treatment plans, and analysis on performance and recovery. To receive treatment, Jane Doe 1 was required to use the Keffer database, and the PII and PHI Jane Doe 1 disclosed was saved on the Keffer system.

77. As a student, Jane Doe 1 was required to disclose personal information to the University and was issued a university email where sensitive, personal information was stored.

78. Because Keffer and the University never implemented the security safeguards needed to protect Jane Doe 1's PII and PHI, Defendant Weiss compromised the PII and PHI belonging to every student whose information was saved by the University and/or Keffer's Athletic

Trainer System database, including, on information and belief, Jane Doe 1's private and personal information.

79. Defendant Weiss compromised all information that was saved in the University and/or Athletic Trainer System databases, including Plaintiff's treatment information, injury information, height, weight, and other highly sensitive information.

80. Jane Doe 1 has received notice from the U.S. Department of Justice Victim Notification System that she was identified as a potential victim in the federal action against Defendant Weiss.¹³

81. After receiving notice from the federal government that read: "If you are receiving this notification, it means that information of yours was found in possession of the defendant,"¹⁴ Jane Doe 1 felt violated, deeply disturbed, humiliated, embarrassed, and extremely emotionally distressed; and is experiencing physical manifestations of the stress and anxiety caused by this egregious violation of her privacy – symptoms that are further exacerbated by the fact that Jane Doe 1 still does not have a full and complete understanding of the data breach and cyber sexual assault perpetrated by Defendant Weiss.

82. This cyber sexual assault invaded Plaintiff's privacy and has devastated her personally and emotionally, as her highly sensitive private information was stolen by an alleged predator under circumstances that were entirely preventable by Defendant University and Defendant Keffer.

83. Upon information and belief, the United States Department of Justice is in the process of notifying thousands of potential victims that their privacy was breached.

¹³ See **Exhibit A**.

¹⁴ *Id.*

84. As a direct result of the negligence, recklessness, and misconduct of the Defendants, Jane Doe 1 and those similarly situated have incurred substantial monetary and emotional damages exceeding \$5,000,000, exclusive of costs, interest, and fees.

DEFENDANTS KEFFER AND LOYOLA UNIVERSITY
CHICAGO FAILED TO PROPERLY PROTECT PLAINTIFF'S AND CLASS
MEMBERS' PII AND PHI

85. Defendants Keffer and University did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted PII and PHI it was maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for approximately 3,330 students and former students.

86. The FTC promulgated numerous guides which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

87. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.¹⁵ The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone

¹⁵ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.¹⁶

88. The FTC further recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

89. Defendants Keffer and Loyola University Chicago failed to properly implement basic data security practices explained and set forth by the FTC.

90. Defendants Keffer's and Loyola University Chicago's failure to employ reasonable and appropriate measures to protect against unauthorized access of PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

91. A systematic, years-long breach such as the ones Defendants Keffer and Loyola University Chicago experienced is also considered a breach under the HIPAA Rules because there is an unauthorized access to PHI that is not permitted under HIPAA.

92. A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." 45 C.F.R. 164.40.

93. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

¹⁶ *Id.*

The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. 45 C.F.R.164.308(a)(6).¹⁷

94. Defendants Keffer's and Loyola University Chicago's data breach was the foreseeable consequence of a combination of insufficiencies that demonstrate that Defendants Keffer and Loyola University Chicago failed to comply with safeguards mandated by HIPAA.

DEFENDANTS LOYOLA UNIVERSITY CHICAGO AND KEFFER FAILED TO COMPLY WITH INDUSTRY STANDARDS

95. Defendants Keffer and Loyola University Chicago did not utilize industry standards appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for approximately 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

96. As explained by the FBI, “[p]revention is the most effective defense against cyberattacks] and it is critical to take precautions for protection.”¹⁸

97. To prevent and detect cyberattacks, including the cyberattack that resulted in this prolific data breach and cyber sexual assault, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of cyberattacks and how it is delivered.

¹⁷ FACT SHEET: Ransomware and HIPPA, U.S. Dept of Health and Hum. Servs., at 4 (July 11, 2016), <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>.

¹⁸ See How to Protect Your Networks from RANSOMWARE, at 3, <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Dec. 20, 2024).

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common cyberware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹⁹
98. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the data breach and cyber sexual assault, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the Internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

¹⁹ *Id.* at 3-4.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....²⁰

99. To prevent and detect cyberattacks, including the cyberattack that resulted in the data breaches and cyber sexual assaults, Defendants Keffer and Loyola University Chicago could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

²⁰ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), <https://www.cisa.gov/news-events/news/protecting-against-ransomware> (last visited Feb. 20, 2025).

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].²¹

100. As described above, experts studying cyber security routinely identify medical facilities as being particularly vulnerable to cyberattacks because of the value of the private information they collect and maintain.

101. Several best practices have been identified that at a minimum should be implemented by institutions such as Defendants Keffer and Loyola University Chicago, including, but not limited to, the following: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

102. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

103. Given that Defendants Keffer and Loyola University Chicago were storing the private information of 150,000 individuals combined, Defendants Keffer and Loyola University Chicago could and should have implemented all the above measures to prevent cyberattacks, along with the two-or multi-factor authentication discussed earlier in this Complaint.

²¹ See *Human-Operated Ransomware Attacks: A Preventable Disaster* (Mar 5, 2020), <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

104. The occurrence, scope and duration of the breach and cyber sexual assaults indicates that Defendants Keffer and Loyola University Chicago failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the exposure of approximately 150,000 students' and former students' PII and PHI, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

DEFENDANTS KEFFER AND LOYOLA UNIVERSITY CHICAGO FAILED TO PROPERLY PROTECT PII AND PHI

105. Defendants Keffer and Loyola University Chicago breached their obligations to Jane Doe 1 and Class Members and were otherwise grossly negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches, cyber-attacks, hacking incidents, and ransomware attacks;
- b. Failing to adequately protect students' private information;
- c. Failing to properly monitor its own data security systems for existing or prior intrusions;
- d. Failing to test and assess the adequacy of its data security system;
- e. Failing to develop adequate training programs related to the proper handling of emails and email security practices;
- f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;
- g. Failing to require a data security system to ensure the confidentiality and integrity of electronic PHI its network created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

- h. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- k. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- l. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- m. Failing to ensure that it was compliant with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);
- n. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);
- o. Failing to ensure that the electronic PHI it maintained is unusable, unreadable, or indecipherable to unauthorized individuals, as Defendants had not encrypted the electronic PHI as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 C.F.R. §164.304 definition of encryption);
- p. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;
- q. Failing to adhere to industry standards for cybersecurity.

106. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendants Keffer and Loyola University Chicago negligently and unlawfully failed to safeguard Plaintiff's and Class Members' private, sensitive information.

107. Defendant Loyola University Chicago was also grossly negligent in its failure to oversee the data security practices of third-party vendor—Keffer—in which it entrusted the sensitive private information of its students and former students.

108. Accordingly, as outlined below, Plaintiff and Class Members have already been severely harmed by this egregious violation of their privacy by Defendant Weiss.

V. CLASS ALLEGATIONS

109. Plaintiff files this lawsuit both individually and as representative of all others similarly situated pursuant to Fed. R. Civ. P. 23 on behalf of the following Class:

All students whose personal data, images, information, social media, or videos were accessed by Weiss without authorization (the “Class Members”).

110. In addition, Plaintiff believes a subclass may be appropriate for all class members who receive notice from the United States Department of Justice as to the likely violation of their privacy and rights by Weiss. Therefore, Plaintiff pleads a subclass as follows:

All students whose personal data, images, information, social media, or videos were accessed by Weiss without authorization and who received a notice letter from the United States Department of Justice as to Weiss (the “DOJ Letter Sub-Class”).

111. Excluded from the Class are: (a) Defendants and any entity or division in which Defendants have a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (b) the Judge to whom this case is assigned and the Judge’s staff; and (c) the attorneys representing any parties to this Class Action.

112. Plaintiff reserves the right to modify or amend the definition of the proposed class and/or sub-classes before the Court determines whether certification is appropriate.

NUMEROSITY – FED. R. CIV. P. 23(A)(1)

113. Law enforcement officials have disclosed the numbers of victims is significant and exceeds one thousand satisfying the numerosity requirement. Although the exact number of Class Members is uncertain at this time, it will certainly be ascertained through appropriate discovery, the number is great enough such that joinder is impracticable.

114. The members of the Class are so numerous and geographically disperse that individual joinder of all members is impracticable.

115. Similarly, Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

116. Class Members are readily identifiable from information and records in the possession of the federal and state authorities, the University, and Keffer.

117. Electronic records maintained by the University and Keffer can confirm the identification of Class Members.

COMMONALITY AND PREDOMINANCE – FED. R. CIV. P. 23(A)(2) AND 23(B)(3)

118. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and the other Class Members. Similar or identical violations, practices, and injuries are involved, and the burden of proof to establish violations of those rights involve uniform, objective questions of fact and law, both for the prosecution and for the defense.

119. The common questions of fact and law existing as to all Class Members predominate over questions affecting only individual class members. The evidence required to advance Plaintiff's and Class Members' claims are the same, common to all; as is true of the

evidence Defendants will likely rely upon in defense of this action. Thus, the elements of commonality and predominance are both met.

120. For example, establishing the facts of how, where, who, when, and through what means the invasions of Plaintiff's and other Class Members occurred are identical.

121. Defendants' actions, inactions, negligence, and recklessness apply commonly to Plaintiff and Class Members.

122. The downloads and invasions by Weiss and the improper conduct accessing private information through unsecure facilities without permission is common to all Class Members and has caused injury to the Plaintiff and Class Members in common manners.

123. The majority of legal and factual issues of the Plaintiff and the Class Members predominate over any individual questions, including:

- (a) Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members private information;
- (b) Whether Defendants Keffer and the University failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the hacking incident and cyber sexual assault;
- (c) Whether Defendants Keffer and the University's data security systems prior to and during the data breach and cyber sexual assault complied with applicable data security laws and regulations;
- (d) Whether Defendants Keffer's and the University's data security systems prior to and during the data breach and cyber sexual assault were consistent with industry standards;
- (e) Whether Defendants Keffer and the University owed a duty to Plaintiff and Class Members to safeguard their private information;
- (f) Whether Defendants Keffer and the University breached their duty to Plaintiff and Class Members to safeguard their private information;
- (g) Whether Defendant University was grossly negligent and/or negligent in its oversight of Defendant Keffer;

- (h) Whether Defendant University or Keffer knew or should have known that their data security systems and monitoring processes were deficient;
- (i) Whether Defendants Keffer and the University owed a duty to provide Plaintiff and Class Members timely notice of the data breach and cyber sexual assaults, and whether Defendants Keffer and the University breached that duty to provide timely notice;
- (j) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;
- (k) Whether Defendants' conduct was negligent or grossly negligent;
- (l) Whether Defendants' conduct was per se negligent;
- (m) Whether Defendants' conduct violated federal laws;
- (n) Whether Defendants' conduct violated state laws;
- (o) Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or punitive damages; and
- (p) Other common questions of fact and law relative to this case that remain to be discovered.

124. Resolving the claims of these Class Members in a single action will provide benefit to all parties and the Court by preserving resources, avoiding potentially inconsistent results, and providing a fair and efficient manner to adjudicate the claims.

125. Predominance does not require Plaintiff to prove an absence of individualized damage questions, or even proof of class wide damage in the aggregate. *Kuchar v. Saber Healthcare Holdings LLC*, 340 F.R.D. 115, 123 (N.D.Ill. 2021) (finding individualized damages questions also do not defeat a predominance finding and noting “when adjudication of questions of liability common to the class will achieve economies of time and expense, the predominance standard is generally satisfied even if damages are not provable in the aggregate.”).

TYPICALITY – FED. R. CIV. P. 23(A)(3)

126. Plaintiff's claims are typical of those of other Class Members because all had their private information compromised as a result of the breach and cyber assault and Defendants' malfeasance.

127. Plaintiff's claims are typical of the Class Members because they are highly similar and the same and related in timing, circumstance, and harm suffered. To be sure, there are no defenses available to Defendants that are unique to individual Plaintiffs. The injury and causes of actions are common to the Class as all arising from the same statutory and privacy interests.

128. In *Halliburton Co. v. Erica P. John Fund, Inc.*, 573 U.S. 258, 276 (2014) the Supreme Court concluded that so long as plaintiffs could show that their evidence is capable of proving the key elements to plaintiffs' claim on a class-wide basis, the fact that the defendants would have the opportunity at trial to rebut that presumption as to some of the plaintiffs did not raise individualized questions sufficient to defeat predominance. "That the defendant might attempt to pick off the occasional class member here or there through individualized rebuttal does not cause individual questions to predominate." *Id.*

129. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

130. The need to conduct additional post certification stage discovery, such as further file review or class member surveys, to eliminate uninjured persons after trial, does not act as a *de facto* bar to certification. *Nixon v. Anthem, Inc.*, 2021 WL 4037824, at *8 (E.D. Ky. Sept 1, 2021) (citing *Young v. Nationwide Mut. Ins. Co.*, 693 F.3d 532, 540 (6th Cir. 2012); *In re Visa Check/MasterMoney Antitrust Litig.*, 280 F.3d 124, 145 (2d Cir. 2001); *Perez v. First Am. Title*

Ins. Co., 2009 WL 2486003, at *7 (D. Ariz. Aug. 12, 2009) (“Even if it takes a substantial amount of time to review files and determine who is eligible for the [denied] discount, that work can be done through discovery.”); *Slapikas v. First Am. Title Ins. Co.*, 250 F.R.D. 232, 250 (W.D. Pa. 2008) (finding class action manageable despite First American's assertion that “no database exists easily and efficiently to make the determination that would be required for each file”).

131. Any remaining disputes on membership or class members damages can be left to a special master's decision. *Whitlock v. FSL Mgmt., LLC*, 2012 WL 3274973, at *12 (W.D. Ky., 2012), *aff'd*, 843 F.3d 1084 (6th Cir. 2016). By placing the validation of injury step at the end of the class trial process, no injured class members are left out, and at the same time, Defendants are not at risk for paying any uninjured class members.

ADEQUACY OF REPRESENTATION – FED. R. CIV. P. 23(A)(4)

132. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that she has no interests that are in conflict with those of the Class Members. In addition, she has retained counsel competent and experienced in complex class action litigation, and she will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and her counsel.

SUPERIORITY OF CLASS TREATMENT – FED. R. CIV. P. 23(B)(3)

133. The class action is superior to any other available procedures for the fair and efficient adjudication of these claims, and no unusual difficulties are likely to be encountered in the management of this class action.

134. The superiority analysis required to certify a class is designed to achieve economies of time, effort and expense, and to promote uniformity of decisions as to persons similarly placed, without sacrificing procedural fairness or bringing about other undesirable results.

135. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable.

136. It would be an unnecessary burden upon the court system to require these individual Class Members to institute separate actions. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

137. Pursuing this matter as a class action is superior to individual actions because:

- (a) Separate actions by Class Members could lead to inconsistent or varying adjudications that would confront Defendants with potentially incompatible standards of conduct;
- (b) Many victims will not come forward without a certified class;
- (c) Final equitable relief will be appropriate with respect to the entire Class as a whole for monitoring, protection, therapy and other equitable forms of relief that may be provided;
- (d) This action is manageable as a class action and would be impractical to adjudicate any other way;
- (e) Absent the class action, individual Class Members may not know if their privacy was invaded; where such images are currently being stored, or are accessible by others; and their injuries are likely to go unaddressed and unremedied; and,
- (f) Individual Class members may not have the ability or incentive to pursue individual legal action on their own.

PARTICULAR ISSUES – FED. R. CIV. P. 23(c)(4)

138. In the event unforeseen issues preclude class certification under Fed.R.Civ.P. 23(b)(3), the case is still appropriate for class certification under Fed.R.Civ.P. 23(c)(4), as to the particular issues of liability.

139. Defendants have acted or refused to act on grounds generally applicable to Plaintiff and the other members of the Class, thereby making declaratory relief, as described below, with respect to the Class as a whole.

COUNT I
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT – 18 U.S.C. § 1030
(Defendant Weiss)

140. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

141. Plaintiffs allege that Defendant Weiss violated the Computer Fraud and Abuse Act.

142. Weiss violated the Computer Fraud and Abuse Act by unlawfully accessing Plaintiffs' private information without authorization.

143. Weiss' actions constituted a violation of the Act because by entering the digital network and extracting sensitive private information of students, he "intentionally accesse[d] a computer without authorization" and/or "exceed[ed] authorized access, and thereby obtain[ed] ... information." 18 U.S.C. § 1030(a)(2)(C).

144. Weiss's actions were deliberate because he knew he was unauthorized and proceeded nevertheless.

145. Under 18 U.S.C. § 1030(g), Plaintiffs may recover damages in this civil action from Weiss along with injunctive relief or other equitable relief.

146. Given the willful violations committed by Weiss, resulting in significant damage, harm, humiliation, and distress to Plaintiffs and other Class Members, Plaintiffs should be awarded all appropriate damages in this matter.

COUNT II
VIOLATIONS OF THE STORED COMMUNICATIONS ACT
18 U.S.C. § 2701 et seq
(Defendants Weiss, Loyola University Chicago, and Keffer)

147. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

148. Plaintiffs allege that Defendants Weiss, Keffer, and University violated the Stored Communications Act.

149. The Stored Communications Act, 18 U.S.C. § 2701 et seq., prohibits the unauthorized access of web-based cloud storage and media accounts such as those at issue and other accounts hosted by Defendants University and Keffer that contain personal, private, and intimate information and communications about and relating to Plaintiffs and others situated similarly to Plaintiffs.

150. Specifically, under 18 U.S.C. § 2701(a), it is unlawful for any person to: (1) intentionally access without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed an authorization to access that facility; and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system.

151. Under 18 U.S.C. § 2702, it is unlawful for a person or entity providing an electronic communication service to the public to knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service or to divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of a subscriber or customer of such service, solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the

contents of any such communications for purposes of providing any services other than storage or computer processing.

152. Plaintiffs' electronic information and communications were in electronic storage and clearly fall within the scope of the statute.

153. Defendant Weiss was not authorized to access or divulge the content of Plaintiffs' private communications by for any purpose.

154. The information, messages, files, and media were accessed by Weiss without authorization.

155. Weiss's access without authorization were deliberate.

156. There is no manner in which Plaintiffs' private information, messages, files, and media could have been obtained without unauthorized access and would not have been obtained without unauthorized access had Defendants University and Keffer not knowingly divulged or permitted access to such information, through Keffer Development other channels, despite knowing that the information would not be protected.

157. Under Section 2707 of the Stored Communications Act, individuals may bring a civil action for the violation of this statute.

158. This law imposes strict liability on violators.

159. The statute provides that a person aggrieved by a violation of the act may seek appropriate relief including equitable and declaratory relief, actual damages or damages no less than \$1,000 punitive damages, and reasonable attorney's fee[s] and other litigation costs reasonably incurred according to 18 U.S.C. § 2707(b)-(c).

160. Defendants' access to and divulging of Plaintiffs' private, personal, and intimate information, messages, files, and media constituted a violation of 18 U.S.C. §§ 2701 and 2702.

161. The University, Keffer, and Weiss knew they did not have authority to access and divulge Plaintiffs' private, personal, and intimate information, messages, files, and media but did so anyway.

162. Defendants' knowing or intentional conduct led to multiple violations of the Stored Communications Act.

163. As a result of these violations, Plaintiffs have incurred significant monetary and nonmonetary damages as a result of these violations of the Stored Communications Act, and Plaintiffs seek appropriate compensation for their damages.

164. Under the statute, Plaintiffs should be granted the greater of (1) the sum of their actual damages suffered and any profits made by the University and Weiss as a result of the violations or (2) \$1,000 per violation of the Stored Communications Act.

165. Given these violations were deliberate, the Court should assess punitive damages against Defendants as well.

166. Plaintiffs should also be granted reasonable attorney fees and costs.

COUNT III
VIOLATION OF TITLE IX, 20 U.S.C. § 1681(A) Et Seq.
(Defendant Loyola University Chicago)

167. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

168. Plaintiffs allege that Defendant Loyola University Chicago violated Title IX, 20 U.S.C. § 1681(A) et seq.

169. Defendant Loyola University Chicago receives federal financial support for its educational programs and is therefore subject to the provisions of Title IX of the Education Act of 1972, 20 U.S.C. § 1681(a), et seq.

170. Title IX mandates that “No person in the United States shall on the basis of sex, be ... subject to discrimination under any education program or activity receiving Federal financial assistance ...”

171. Each Plaintiff and Class Member is a “person” under the Title IX statutory language.

172. Weiss specifically targeted women in his unwanted invasions of privacy and his misconduct is discrimination on the basis of sex.

173. Defendant Loyola University Chicago, under Title IX, is obligated to investigate allegations of sexual harassment.

174. Defendant Loyola University Chicago was aware of the sensitive nature of the private and personal information of Plaintiffs to which Weiss was able to access.

175. Defendant Loyola University Chicago acted with deliberate indifference to sexual harassment by:

- a. Failing to protect Plaintiffs and others as required by Title IX;
- b. Neglecting to adequately investigate and address the complaints regarding the deeply sensitive information Plaintiffs provided;
- c. Failing to institute corrective measures to prevent Weiss from sexually harassing students; and
- d. Failing to adequately investigate the other multiple acts of deliberate indifference.

176. Defendant Loyola University Chicago acted with deliberate indifference as their lack of response to the sexual harassment was clearly unreasonable in light of the known circumstances.

177. Defendant Loyola University Chicago's failure to promptly and appropriately protect, investigate, and remedy and respond to the sexual harassment of women has effectively denied them equal educational opportunities at the University, including access to medical care and sports training.

178. At the time the Plaintiffs received some medical and/or athletic training services from the University, they did not know the Defendant failed to adequately consider their safety.

179. As a result of Defendant Loyola University Chicago's deliberate indifference, Plaintiffs have suffered loss of educational opportunities and/or benefits.

180. Plaintiffs have incurred, and will continue to incur, attorney's fees and costs of litigation.

181. At the time of Defendants' misconduct and wrongful actions and inactions, Plaintiffs were unaware, and or with reasonable diligence could not have been aware, of Defendants' institutional failings with respect to their responsibilities under Title IX.

182. Defendant Loyola University Chicago maintained a policy and/or practice of deliberate indifference to protection of female student athletes.

183. Defendant's policy and/or practice of deliberate indifference to protection against the invasion of privacy for female athletes created a increased risk of sexual harassment.

184. Despite being able to prevent these privacy violations and acts of harassment, Defendant failed to do so.

185. Because of the Defendant Loyola University Chicago's policy and/or practice of deliberate indifference, Plaintiffs had their privacy invaded and were sexually harassed by Weiss.

186. Plaintiffs should be awarded all such forms of damages in this case for Defendant Loyola University Chicago's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

COUNT IV
VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 - UNREASONABLE SEARCH AND SEIZURE
(Defendant Weiss)

187. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

188. Plaintiffs allege Defendant Weiss violated their civil rights under 42 U.S.C. § 1983 and the Fourth Amendment of the U.S. Constitution.

189. Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this action, and acted under color of state law to deprive Plaintiffs of their "rights, privileges or immunities secured by the Constitution and laws" of the United States, 42 U.S.C. § 1983, specifically their Fourth Amendment right to be free warrantless and unreasonable searches and seizures.

190. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally searched and seized Plaintiffs' private information without their consent, without a warrant, without probable cause or reasonable suspicion, and without any lawful basis or justification, in violation of Plaintiffs' clearly established rights under the Fourth Amendment.

191. The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."

192. It is well settled that the Fourth Amendment's protection extends beyond the sphere of criminal investigations. *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 755 (2010) (citing *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 530 (1967)).

193. "The [Fourth] Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government," without regard to whether the government actor is investigating crime or performing another function." *Id.* (quoting *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602, 613-614 (1989)).

194. Plaintiffs had a reasonable and legitimate expectation of privacy in their private, personal, and intimate information and images.

195. Acting under color of law, Defendant Weiss violated Plaintiffs' clearly established right not to have their private, personal, and intimate information and images. accessed, searched, viewed, and seized when he searched and seized Plaintiffs' private, personal, and intimate information and images without a warrant, without reasonable suspicion, without probable cause, and without any lawful basis, justification or need to support such an intrusion on Plaintiffs' reasonable and legitimate expectation of privacy in that information.

196. Defendant Weiss's search and seizure of Plaintiffs' personal information was per se unreasonable under the Fourth Amendment.

197. Defendant Weiss' search and seizure of Plaintiffs' private, personal, and intimate information and images was unjustified at its inception and was not related in scope to any circumstances that would justify the search and seizure in the first place.

198. Defendant Weiss is not entitled to qualified immunity because Plaintiffs' rights under the Fourth Amendment not to have their personal information searched and seized by him without a warrant, without permission, and without any lawful basis or justification, was obvious

and clearly established when Weiss accessed Plaintiffs' private information, such that no reasonable person in Weiss's position would believe that the act of searching and seizing Plaintiffs' private information was lawful under the specific circumstances presented, and Weiss had fair warning under the law as it existed at the time of his actions that those actions obviously violated Plaintiffs' rights under the Fourth Amendment.

199. As a direct and proximate result of Weiss's violation of Plaintiffs' Fourth Amendment rights, Plaintiffs have suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

200. Plaintiffs should be awarded all such forms of damages in this case for Weiss's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

COUNT V
VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 - DUE PROCESS/BODILY INTEGRITY
(Defendant Weiss)

201. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

202. Plaintiffs are alleging Defendant Weiss violated their civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

203. Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this action, and acted under color of state law to deprive Plaintiffs of their "rights, privileges or immunities secured by the Constitution and laws" of the United States, 42 U.S.C. § 1983, specifically their Fourteenth Amendment equal protection right to be free from sexual harassment in an educational setting, and their Fourteenth Amendment due process right to be free

from violation of bodily integrity. *West v. Atkins*, 487 U.S. 42, 49-50 (1988) (quoting *Lugar v. Edmondson Oil Co.*, 457 U.S. 922, 936 n. 18 (1982)).

204. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right to be free from sexual abuse at the hands of a state employee was protected by the Due Process Clause of the Fourteenth Amendment, such that he knew his actions in accessing Plaintiffs' Plaintiffs' private, personal, and intimate information and images violated Plaintiffs' fundamental right of due process.

205. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in actions which violated Plaintiffs' right of bodily integrity, in violation of the Due Process Clause.

206. Weiss's actions were malicious, intentionally harmful, and were taken with deliberate indifference, and were so outrageous as to shock the contemporary conscience.

207. As a direct and proximate result of Weiss's violation of Plaintiffs' Fourteenth Amendment rights, Plaintiffs have suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

208. Plaintiffs should be awarded all such forms of damages in this case for Weiss's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

COUNT VI
VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 - EQUAL PROTECTION
(Defendant Weiss)

209. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

210. Plaintiffs are alleging Defendant Weiss violated their civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

211. Weiss's deliberate and intentional actions in accessing Plaintiffs' personal, private, and intimate images and information constituted sexual harassment and abuse because Weiss accessed Plaintiffs' highly sensitive, private, and personal information, data, and media for his own personal and sexual purposes.

212. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right to be free from gender discrimination, including sexual harassment and abuse at the hands of a state employee, was protected by the Equal Protection Clause of the Fourteenth Amendment, such that Weiss knew his actions in accessing Plaintiffs' personal, private, and intimate images and information violated Plaintiffs' rights under the Fourteenth Amendment.

213. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in sexual harassment and sexual abuse, in violation of the Equal Protection Clause.

214. As a direct and proximate result of Weiss's violation of Plaintiffs' Fourteenth Amendment rights, Plaintiffs have suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

215. Plaintiffs should be awarded all such forms of damages in this case for Weiss's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

COUNT VII
VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 - DUE PROCESS/DEPRIVATION OF PROPERTY
(Defendant Weiss)

216. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

217. Plaintiffs allege that Defendant Weiss violated their civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

218. Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this action, and acted under color of state law to deprive Plaintiffs of their "rights, privileges or immunities secured by the Constitution and laws" of the United States, 42 U.S.C. § 1983, specifically their Fourteenth Amendment due process right to be free of deprivations of property without due process

219. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right not to be deprived of one's property without due process was protected by the Due Process Clause of the Fourteenth Amendment, such that he knew his actions in accessing and misappropriating Plaintiffs' private, personal, and intimate information and images violated Plaintiffs' fundamental right of due process.

220. Plaintiffs and others similarly situated had a protected property interest in their personal, private, intimate, and confidential information.

221. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in actions which violated Plaintiffs' right not to be deprived of their personal property, in violation of the Due Process Clause.

222. Weiss' actions were malicious, intentionally harmful, and were taken with deliberate indifference, and were so outrageous as to shock the contemporary conscience.

223. As a direct and proximate result of Weiss' violation of Plaintiffs' Fourteenth Amendment rights, Plaintiffs have suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

224. Plaintiffs should be awarded all such forms of damages in this case for Weiss' conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

RELIEF

WHEREFORE, Plaintiff prays this Court grant the following relief:

- a. Enter a judgment encompassing the relief requested above, plus significant compensatory damages exceeding \$5,000,000.00 together with costs, interest and attorney fees, against Defendants, and such other relief to which they are entitled;
- b. An order certifying the proposed Class and Subclasses; designating Plaintiff as the named representative of the respective Class Members; and appointing her counsel as Class Counsel;
- c. All such equitable relief as the Court deems proper and just, including but not limited to, declaratory relief;
- d. Award Plaintiff costs, attorney fees as well as interest from the date of Judgment until paid; and
- e. Grant such further relief as is agreeable to equity and good conscience.

JURY DEMAND

For all triable issues, a jury is hereby demanded.

Respectfully Submitted,

/s/ Edward A. Wallace

Edward A. Wallace

Jacob Podell

WALLACE MILLER

150 North Wacker Drive, Suite 1100

Chicago, IL 60606
T: 312.261.6193
F: 312.275.8174
E: eaw@wallacemiller.com
jpodell@wallacemiller.com

Counsel for Plaintiff and the Proposed Class